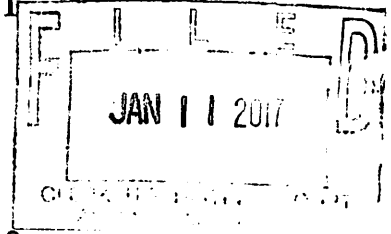


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

7123 DRYBURGH COURT
SPRINGFIELD, VA 22152

Case No. 1:17-SW-9

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC § 922(a)(1)(A)	Dealing in firearms without a license

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA
AUSA F. Nathaniel Smith, III

Applicant's signature
Zachary D. Mikkelson, ATF Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/11/2017

City and state: Alexandria, Virginia

/s/ JFA
John F. Anderson
United States Magistrate Judge
Honorable John F. Anderson
Printed name and title
U.S. MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is listed below:

7123 Dryburgh Court, Springfield, VA 22152

This building is described as a two story detaching dwelling designed as a single family home.

The lower level is brick and the upper level is sided. The address number "7123" is painted in black numbers on a white background on the curb in front of the dwelling. The driveway is constructed of concrete and the mailbox is white with a dark colored post. The right side of the lower level extends further than the upper level of the dwelling.

ATTACHMENT B

1. All records and information related to violations of 18 U.S.C. § 922(a)(1)(A), violations of 18 U.S.C. § 922(g), and violations of 18 U.S.C. § 922(n), specifically:
 - a. Any records and information involving the purchase, advertising, and sale of firearms
 - b. Any records and information involving the business of dealing in firearms
 - c. Any records and information related to the sale of firearms to Anthony FERNANDEZ MEDRANO
 - d. Any records and information related to the sale of firearms to Kyle LUSBY
 - e. Any records and information related to firearms inventory, transfers, acquisitions, and dispositions of firearms and firearms parts.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. records of or information about Internet Protocol addresses used by the
COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including
firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
web pages, search terms that the user entered into any Internet search engine, and
records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this
attachment.

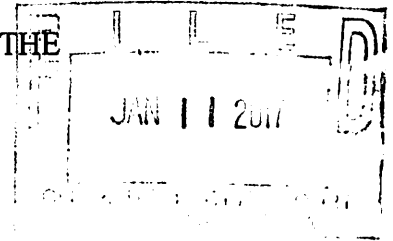
As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF

THE RESIDENCE OF HAINING DU
7123 DRYBURGH COURT,
SPRINGFIELD, VA 22152

1:17-sw-9

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Zachary D. Mikkelson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") since 2015. Prior to my appointment with the ATF, I was a sworn law enforcement officer with the Commonwealth of Virginia for six years. I am currently assigned to the ATF Falls Church Group II Field Office.

2. In my capacity as a law enforcement officer, I have investigated individuals for the illegal possession and use of firearms, illegal possession and distribution of controlled substances, for committing violent crimes, and for violations involving dealing in the business of firearms without a valid license.

3. The facts and information contained in this affidavit are based upon my personal knowledge, information obtained from federal and state law enforcement officers, and information obtained from interviews and analysis of reports.

4. This affidavit contains information necessary to support probable cause. The information contained in this affidavit is not intended to include each and every fact and matter observed by me or known to the government.

PROBABLE CAUSE

5. On September 15, 2016 Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) Special Agent (SA) Zachary Mikkelson received information that Haining DU had been reported on number Multiple Sales Reports in the previous six months. Multiple Sales reports, which are reports required to be generated by Federal Firearms Licensees (FFLs) pursuant to 18 USC 923(g)(3)(A) when an individual purchases more than one handgun from the same FFL in five business days or less. These reports are required to be submitted to ATF, and SAs have access to these reports which are compiled by the National Tracing Center (NTC). SA Mikkelson reviewed these reports in this case, which indicated that DU had purchased 25 firearms since March 23, 2016. The majority of these firearms were small caliber, semi-automatic pistols. Further investigation revealed that DU had purchased an additional 5 firearms on September 15, 2016. DU had also purchased numerous firearms of identical make, model, and caliber. In my training experience, purchases of multiple inexpensive firearms of small caliber, semi-automatic pistols are not typically acquired for a buyer's personal collection and are generally indicative of a scheme to resell the firearms which would require a valid license.

6. On September 23, 2016 at approximately 0654 hours, SA Mikkelson and SA Kerwin made contact with DU at his residence, 7123 Dryburgh Court, Springfield, Virginia 22152, and proceeded to interview him about his recent firearms purchases. DU was questioned specifically regarding seven of the firearms that he had purchased. DU was able to present four of the firearms requested. DU presented "bills of sale" for the other three firearms which were

all Ruger model LCP, .380 caliber pistols. DU indicated that he completes a bill of sale for each firearm that he sells, that he checks identification of each purchaser, and that he only sells to residents of Virginia. DU stated that he refuses to sell the firearm if they will not complete the bill of sale. DU indicated that he purchases multiple firearms at one time because it saves him money in transfer fees and that he uses VAguntrader.com and armslist.com in order to advertise the firearms that he sells. DU does not operate a physical office for the sale of his firearms, and while at his residence at 7123 Dryburgh Court in Springfield, Virginia, he produced a "Bill of Sale" for three of the firearms that he had sold. Based on this information, it is believed that DU also keeps copies of the bills of sale for other firearms that he sells at that residence.

7. DU estimated that he had purchased approximately 30 firearms in the last year and that he had sold approximately half of the firearms that he had purchased. DU stated that he does not make much of a profit from selling the firearms, especially after all the time that he spends conducting the purchases and sales of the firearms is taken into account. DU stated that he does not sell firearms for a living and indicated that he has a primary occupation that he devotes most of his time to.

8. DU indicated during the interview that he only sold firearms when he purchased them and then realized that he did not like them. SA Mikkelson confronted him with the fact that he purchased a Ruger, model LCP, .380 caliber pistol on March 23, 2016 and DU indicated that he had sold that firearm on March 26, 2016. SA Mikkelson then asked why DU had proceeded to purchase five more of the exact same model of pistol of which he had sold at least two. The only answer that DU could provide was that he did not like the way they "racked." In my training and experience, the explanation DU gave is not credible because the process used to manufacture firearms generally uses a method involving the assembly of standardized parts;

therefore, the same make and model of firearm typically operate in like manner and contain like specifications making it very unlikely that two firearms of the same make and model will function with any noticeable difference.

9. In addition to the information that demonstrates that DU is buying firearms and then quickly reselling them, there is also reason to believe that DU is reselling at least some of those firearms to prohibited persons. A prohibited person is someone who is unable to acquire a firearm lawfully. For example, one bill of sale indicated that one of the firearms that DU purchased on March 23, 2016 was sold to Kyle LUSBY on March 26, 2016. An initial check into LUSBY's criminal history indicates that he was under indictment for a felony at the time that he purchased the firearm and was later convicted of that felony on May 18, 2016. LUSBY is also currently on probation in Arlington County and prohibited from possessing a firearm as a condition of his probation.

10. Another of DU's bills of sale indicated that he sold two Ruger model LCP, .380 caliber pistols to Anthony FERNANDEZ MEDRANO, but did not indicate the date on which the sale was completed. The ATF Form 4473 related to DU's transaction indicates that both of the firearms sold to FERNANDEZ MEDRANO were purchased on June 3, 2016. An initial search of FERNANDEZ MEDRANO's criminal history indicates that he was under indictment for a felony on June 3, 2016, and thus under indictment on the date that he purchased the firearm from DU in violation of 18 USC 922(n), which prohibits persons under indictment for a felony from purchasing a firearm. FERNANDEZ MEDRANO is also currently on probation in Arlington County and prohibited from possessing a firearm as a condition of his probation.

11. Contact with FERNANDEZ MEDRANO confirms that multiple transactions with DU occurred. On October 13, 2016, FERNANDEZ MEDRANO was interviewed at the Arlington County Probation and Parole Office. FERNANDEZ MEDRANO admitted that he had purchased three firearms from DU and estimated that his most recent purchase from DU was approximately two to three months ago. FERNANDEZ MEDRANO stated that he communicated with DU using the email address antfernandez715@gmail.com. FERNANDEZ MEDRANO stated that he met DU at the Huntington Metro Station to conduct the transactions and that they only communicated using email. FERNANDEZ MEDRANO stated that they only met twice and that he purchased a total of three firearms. FERNANDEZ MEDRANO stated that all three firearms were semi-automatic pistols. FERNANDEZ MEDRANO stated that he purchased a .380 the first time for approximately \$300 and on the second meeting he purchased another .380 and an unknown type (possible a Springfield XD .40) for approximately \$550 for both.

12. FERNANDEZ MEDRANO denied asking DU to acquire any specific firearms for him. FERNANDEZ MEDRANO stated that DU told him that he had other similar firearms for sale at their first meeting. FERNANDEZ MEDRANO denied currently possessing any of the firearms that he had purchased. He stated that he had sold them all to unknown parties using armslist.com. FERNANDEZ MEDRANO stated that DU told him he had "plenty" of the .380s for sale. FERNANDEZ MEDRANO denied telling DU that he was on probation and admitted that he was selling the firearms for \$100 over his purchase price in order to make a profit. FERNANDEZ MEDRANO stated that DU was the only person that he had purchased a firearm from. FERNANDEZ MEDRANO also stated that he utilized the same email account (antfernandez715@gmail.com) in order to arrange the sale of the firearms.

13. After learning on DU's sales to LUSBY and FERNADEZ MENDRANO, DU was again interviewed on September 27, 2016 and was confronted with the information that some of the firearms that he had sold were to a prohibited person. DU only provided limited information on the transactions, but DU did admit that he had conducted multiple transactions with FERNANDEZ MEDRANO. DU, however, refused to go into further detail about the transactions. DU was informed at this interview that it is generally a violation of federal law to engage in the business of selling firearms without a license.

14. Despite knowing that it is violation of federal law to engage in the business of selling firearms without a license, DU's purchases of firearms continued unabated. On September 28, 2016 SA Mikkelson received information from a Federal Firearm Licensee (FFL) that DU had purchased an additional firearm (Walther, model PPQ, 9mm pistol). So far, SA Mikkelson has been able to obtain records of 45 firearms that have been purchased by DU since March 23, 2016. Of the 44 firearms purchased by DU, all but two were semi-automatic pistols. The majority of these were less expensive models and those typically associated with purchase for resale. And by DU's own admission in an interview with SA Mikkelson, he had sold half of these firearms already. Indeed, in my training and experience, very few of the firearms models being purchased by DU are typically collected in large number by firearms enthusiasts. Based on this information, I submit that there is probable cause to believe that DU is engaging in the business of purchasing and selling firearms without a valid license to do so in violation of 18 USC 922(a)(1)(A) and that there is probable cause to believe that records of DU's transactions with customers, including transactions with prohibited persons, are located at his residence at 7123 Dryburgh Court, Springfield, Virginia 22152, where SA Mikkeleson interviewed him previously and where DU had previously produced firearms that he had recently purchased and

records of firearms that he had sold. As a result, there is probable cause for a search warrant to be issued for DU's residence to locate records of purchases and sales of firearms.

15. On December 21, 2016 SA Mikkelson located a listing on armslist.com for a pistol, manufactured by Hechler & Koch, model VP9, 9mm for \$580. Based on purchases made by DU, SA Mikkelson knew that DU had purchased the same model of firearm from Sharpshooters LLC. on December 18, 2016. The posting advertised the firearm as:

- a. "Brand new in box, everything included (2 mags, lock and etc). No wear marks or scratches. Please refer to photos. Local and cash only. VA ID required."

16. Utilizing an armslist.com account created by a CI, SA Mikkelson contacted the "seller" through armslist.com and asked if the firearm was still available. The CI then received an email from durealty@gmail.com stating that the firearm was still available and that he could meet to sell it outside of Sharpshooters in Lorton, VA. The seller was asked to provide a phone number and provided the number 202-870-1245, which is a number that DU had previously used to contact SA Mikkelson during the investigation.

17. As part of this interaction, DU provided a "bill of sale" in one of the emails that was identical to the documents provided to SA Mikkelson during the interview on September 23, 2016. Task Force Officer (TFO) Joey Davis, acting in an undercover capacity also contacted DU through armslist.com in reference to a separate listing that DU had posted for a Springfield, model XDS, 9mm pistol. This description matched a firearm transferred to DU on November 20, 2016. During this interaction, DU provided the same "bill of sale" form to TFO Davis.

18. On December 22, 2016, TFO Davis, again acting in an undercover capacity, met with DU in the parking lot of Sharpshooters LLC. in Lorton, VA and purchased a Springfield,

model XDS, 9mm pistol, bearing serial number S3703606. This serial number matched the serial number recorded on an ATF Form 4473 from a purchase made by DU on November 20, 2016. During this transaction, DU provided TFO Davis with the same “bill of sale” that he had provided during their email interaction. At the conclusion of the transaction, DU provided one copy of the “bill of sale” to TFO Davis, and retained the other copy.

19. Additionally, Industry Operations Investigator (IOI) Patrick Hoover, conducted a search of the Federal Licensing System (FLS) for the name “DU, Haining” and found no results for current Federal Firearms Licenses or applications for Federal Firearm Licenses. IOI Hoover also conducted a search of FLS using DU’s date of birth and found no results in Virginia.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

- e. Based on actual inspection of other evidence related to this investigation, including internet postings on armslist.com, I am aware that computer equipment was used to generate, store, and print documents used in the dealing firearms without a license scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and

events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

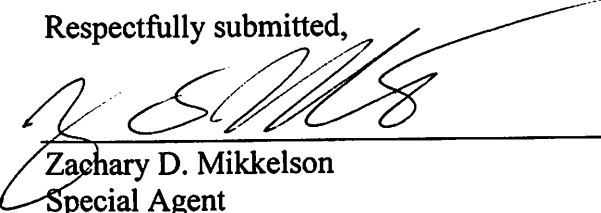
Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would

authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


CONCLUSION

24. I submit that this affidavit supports probable cause that there are additional records located at the residence of DU and that a search will yield further evidence that DU engaged in the business of selling firearms without a license in violation of Title 18 United States Code, Section 922(a)(1)(A), and the purchase of firearms by prohibited persons in violation of Title 18 United States Code, Sections 922(g), and 922(n).

Respectfully submitted,


Zachary D. Mikkelson
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me on January 11, 2017:

/s/ 
John F. Anderson
The Honorable John F. Anderson
United States Magistrate Judge
United States Magistrate Judge